(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－304333

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]	識別記号	FI		
H04N	7/167	H04N	7/167	Z
H04L	9/14	H04L	9/00	641

審査請求　未請求　請求項の数8　ＯＬ　（全 17 頁）

(21)出願番号　特願平10－43111

(22)出願日　平成10年(1998) 2月25日

(31)優先権主張番号　特願平9－46529

(32)優先日　平9 (1997) 2月28日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

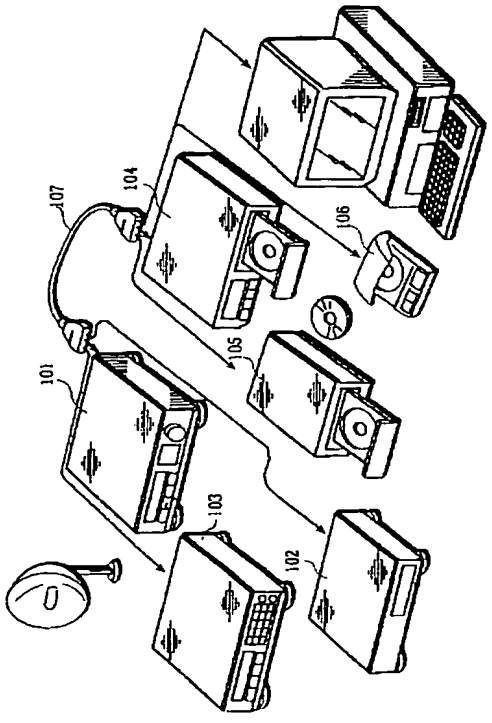
(74)代理人　弁理士　中島　司朗

(54)【発明の名称】　デジタル著作物の著作権保護のための暗号技術利用プロトコルを複数から選択して使用する情報機器

(57)【要約】

【課題】　認証機器、証明機器の組み合わせによって、認証処理・証明処理が正当に行えないという不合理の発生を防止する。

【解決手段】　認証機器及び証明機器は自機の機種情報を互いに相手側に通知する。認証機器は、相手側から通知された証明機器側の機種情報に対応する認証方法を決定して、決定した認証方法に対応するチャレンジデータを作成して相手側に送信する。証明機器は、相手側から通知された認証機器側の機種情報に対応する証明方法を決定して、相手側からチャレンジデータが送信されると相手側から通知された認証機器側の機種情報に対応する証明方法を決定する。そして決定した証明方法を用いてチャレンジデータに対して証明処理を行い、レスポンスデータを作成して相手側に送信する。認証機器は相手側からレスポンスデータが返信されて来ると、そのレスポンスデータの認証を行う。



1

【特許請求の範囲】

【請求項１】　複数の情報機器からなり、複数の暗号技術利用プロトコルの利用が可能な通信システムにおいて各情報機器は、

自機の機種が複数の暗号技術利用プロトコルのうちどれとどれを利用することができる機種であるかを示す機種情報を通信すべき相手側情報機器に通知する通知手段と、

相手側情報機器から機種情報が通知されると、通知された機種情報と自機の機種情報との組み合わせから情報機器間で用いるべき何れか一つの暗号技術利用プロトコルを決定する決定手段と、

前記自機の機種情報に対応する１以上のプロトコルに基づいて相手側機器と通信する１以上のプロトコル対応通信部を有し、その中の一つに決定された暗号技術利用プロトコルを用いて通信を行わせる通信手段とを備えることを特徴とする通信システム。

【請求項２】　前記通信システムにはn種(nは2以上の整数)の機種が存在し、

前記決定手段はn種の機種から任意の2種を選んだnC2個の機種情報の組み合わせと、各組み合わせにおいて用いるべき暗号技術利用プロトコルを示すプロトコル対応情報を対応づけたテーブルを記憶するテーブル記憶部と、

n種の機種のうち、自機に合致するものの機種情報を記憶する機種情報記憶部と、

相手側機器から機種情報が通知されると、テーブル記憶部が記憶しているテーブルにおいて機種情報記憶部が記憶している機種情報と、相手側機器から通知された機種情報との組み合わせに対応づけられたプロトコル対応情報が示す暗号技術利用プロトコルを前記一のプロトコルと決定する決定部とを備え、

前記１以上のプロトコル対応通信部は、

決定部が決定した暗号技術利用プロトコルを用いて通信を行うことを特徴とする請求項１記載の通信システム。

【請求項３】　前記暗号技術利用プロトコルは、相手側認証プロトコルであり、

前記通信システムにおける何れか一つの情報機器に備えられたプロトコル対応通信部は決定部が決定した相手側認証プロトコルにより相手側機器に正当性を証明させ、その証明結果に基づいて相手側機器が正当な情報機器であるか否かを判定する認証部と、

正当な情報機器であると判定された場合のみ、保護対象となるデータを相手側情報機器に送信する送信部とを備えることを特徴とする請求項２記載の通信システム。

【請求項４】　前記テーブル記憶部は、

nC2個の機種情報の組み合わせにおいて用いるべき相手側認証プロトコルを対応づけたテーブルを複数種別記憶しており、

複数のテーブルのうち第１のテーブルには、

機種情報の組み合わせにおいて用いるべき相手側認証プロトコルとして安全性が高い相手側認証プロトコルを特定するプロトコル対応情報が記述され、

第２のテーブルには、

機種情報の組み合わせにおいて用いるべき相手側認証プロトコルとして処理速度が高い相手側認証プロトコルを特定するプロトコル対応情報が記述されており、

前記情報機器に備えられた決定手段はこれから行うべき通信における安全性及び処理速度の何れか一方を考慮して、テーブル記憶部が記憶しているテーブルのうち一つを選択すると共に、どのテーブルを選択したかを相手側に通知する選択部を備え、

前記決定部は、

テーブル記憶部に記憶されているテーブルのうち、選択部が選択して、相手側に通知したテーブルにおける相手側認証プロトコルを決定することを特徴とする請求項３記載の通信システム。

【請求項５】　複数の相手側認証プロトコルには複数のチャレンジ・レスポンス型認証プロトコルがあり、

複数のチャレンジ・レスポンス型認証プロトコルには公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルと、秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルとがあり、

前記第１種別のテーブルには、

安全性が高いチャレンジ・レスポンス型認証プロトコルとして公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルを示すプロトコル対応情報が記述され、

前記第２種別のテーブルには、

処理速度が早いチャレンジ・レスポンス型認証プロトコルとして秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルを示すプロトコル対応情報が記述されており、

前記１以上のプロトコル対応通信部には、

公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルに基づいて通信するものと、秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルに基づいて通信するものが存在することを特徴とする請求項４記載の通信システム。

【請求項６】　公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルに基づいて通信するプロトコル対応通信部における認証部は、

乱数をチャレンジデータとして生成して相手側に送信するチャレンジデータ作成部と、

相手側からレスポンスデータが返信されてくると、そのレスポンスデータを所定の公開鍵データに基づいて復号する復号部と、

復号部による復号結果に基づいて、相手側機器の正当性を判定する判定部とをを備え、

秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルとに基づいて通信するプロトコル対応通信部における認証部は乱数をチャレンジデータとして生成して相手

側に送信するチャレンジデータ作成部と、
相手側からレスポンスデータが返信されてくると、そのレスポンスデータを所定の秘密鍵データに基づいて復号する復号部と、
復号部による復号結果に基づいて、相手側機器の正当性を判定する判定部とを備えることを特徴とする請求項５記載の通信システム。

【請求項７】　複数の相手側認証プロトコルには複数のチャレンジ・レスポンス型認証プロトコルがあり、
複数の相手側認証プロトコルには公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルと、秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルとがあるを備えることを特徴とする請求項３記載の通信システム。

【請求項８】　複数の相手側認証プロトコルには、
一方向認証方法時系列認証方式があることを特徴とする請求項３記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信リンクで結合された複数の機器においてディジタルデータを通信する際に、その通信リンク上のディジタルデータを保護するために暗号技術を利用した通信システムに関する。

【０００２】

【従来の技術】映画等の映像著作物は、ディジタル化され、情報圧縮された状態で利用されることが主流になる傾向にある。デジタル化･圧縮化された映像著作物は、画質の劣化が殆どなく、視聴者は、常に最高の画質にて映像著作物を鑑賞することができる。またアナログ状態の映像著作物は、ダビングを何度も繰り返すとその画質が著しく劣化するのに対し、デジタル化された映像著作物は、ダビングを何度繰り返しても画質の劣化が生じない。

【０００３】見方を変えると、デジタル化された映像著作物は不法なデッドコピーや不正改変がアナログ状態のそれと比べてすこぶる容易であり、著作権侵害行為に対して無防備な状態にさらされているといえる。デッドコピー及び不正な改変が行われ、再配布されると著作権者は多大な打撃を被る。それ故に、映像著作物の著作権者は、映像著作物のデジタル化に慎重な態度を示している。これらの背景から、映像著作物のデジタル化においては、映像著作物の著作権をその侵害行為から防御するかが大きな論点とされている。

【０００４】ここでデッドコピーは、映像著作物を記録した記録媒体を再生する映像再生装置と、再生された映像著作物を入力してこれを記録媒体に記録する情報記録装置とを接続することによりなされる。また不正改変行為は、映像著作物を記録した記録媒体を再生する映像再生装置と、再生された映像著作物を入力してこれを一旦ハードディスクに蓄積し、後日これを編集する映像編集装置とを接続することによりなされる。

【０００５】これらの侵害行為を抑止するには、映像著作物を再生する側の映像再生装置が、情報記録装置及びディジタル情報複製装置を始めとする不正な機器への流出するのを防ぐしかない。不正機器への流出を防ぐには、映像再生装置が通信リンクに接続された際、通信リンクを介して映像再生装置と接続された相手側機器の正当性を確認すればよい。

【０００６】相手側の正当性を確認する技術の最も代表的なものは相手認証技術を用いる技術である。これは基本的にはデータを送出する機器が受信する機器の正当性を認証し、正当な受信機器であることが確認できたときのみにデータを送信することによりデータが不正な機器に受信されることを避ける。この場合の受信機器のように自らの正当性を証明する側を証明機器と呼び、またこの場合の送信機器のように相手の正当性を確認する側を認証機器と呼ぶ。

【０００７】前述の光ディスク記録再生に関わる機器のような場合、光ディスク関連機器の間で著作権保護のために一定の基準が設けられる。この時、ある機器はこの基準を満たすものであるかどうかが問題となる。従って「正当性を認証する」とは「所定の規格に準拠することかどうかを判別する」という意味となる。従来の技術の一例として国際標準規格ISO/IEC9798-2に記載される暗号技術を用いた一方向認証方法がある。この認証方法は証明機器が証明鍵と呼ばれる秘密のデータを持つことを、その鍵自身を知らせることなく認証機器に対して証明することを基本としている。そのためにまず認証機器があるデータを選びこれを証明機器に対して投げかける。この行為をチャレンジと呼び、上記規格において投げかけられるデータは64bitと規定されている（このデータをチャレンジデータと呼ぶ。）。

【０００８】一方、証明機器は暗号変換アルゴリズムと前記証明鍵とを保有しており、両者を用いて前記チャレンジデータを暗号化する。この暗号化は、たとえ暗号値及びチャレンジデータの両者を用いても、前記証明鍵が導出できないことが保証されている。このように暗号化されたデータをレスポンスとして認証機器に対して返す。このレスポンスを受信した認証機器は前記暗号変換に対応する復号変換アルゴリズムと検証鍵を有している。そして、レスポンスデータを前記検証鍵を用いて自己の持つ復号変換アルゴリズムによって復号する。復号後、復号結果をチャレンジデータと比較し、前記復号結果がチャレンジデータと一致すれば受信側機器は相手側が正規の証明鍵を持つものと判断し、証明機器の正当性を認証する。一方向認証は一方の側がその正当性を他方に証明した時点で終了するが、上記手順を認証機器と証明機器を入れ替えて再度行うことにより、更に相手側の正当性を確認してもよい（これは双方向認証と呼ばれる。）。

【０００９】認証技術において用いられる暗号変換には秘密鍵暗号変換と公開鍵暗号変換がある。レスポンスデータ作成と、レスポンスデータの検証のために鍵を用いるものとする。そしてレスポンスデータの作成のために用いる鍵を証明鍵と呼び、レスポンスデータの検証のために用いる鍵を検証鍵と呼ぶものとする。この場合秘密鍵暗号変換では、上記の証明鍵と検証鍵とは共通のもので良い。そのため、秘密鍵暗号変換を用いる場合検証鍵、証明鍵の何れか一方の漏洩は許されない。

【００１０】公開鍵暗号変換は、上記証明鍵と検証鍵は異なるものを用いる。このため証明鍵は秘密にしておかねばならないが、検証鍵は秘密にする必要がない（秘密にしておかねばならない鍵を秘密鍵といい、秘密にする必要がない鍵を公開鍵という。）。秘密鍵暗号変換をコンピュータのソフトウェアによって実現する場合、処理時間が短くできるという利点がある。またハードウェアで実現する場合にはハードウェア量が少なくなるという利点がある。一方、証明鍵のみならず検証鍵も秘密でなければならないというのは欠点でもある。いま仮に証明機器の証明鍵を別のものに取り替えるものとしよう。このとき認証機器にある検証鍵も同時に取り替える必要がある。ところが証明機器の変更された証明鍵に対応する検証鍵を通信リンクを介して伝送することはできない。なぜならば通信リンク上のデータは不正にコピーされるという前提に立っており、その秘密性は守られないからである。従って証明機器の証明鍵を取り替えることは困難となる。つまり、全システムが同じ種類の秘密（証明鍵または検証鍵）を持つことになる。従ってもし万一この秘密が破られると全システムの秘密が破られることになる。

【００１１】一方、公開鍵暗号変換には通常大量の計算量が必要となり、一般のコンピュータのソフトウェアで実現するためには処理時間がかかることはよく知られている。またこれを専用のハードウェアで実現する場合は必要となるハードウェア量が多くなる。これらのことは公開鍵暗号変換の短所である。公開鍵暗号変換を用いたチャレンジレスポンス型の認証方法を用いる場合、レスポンスデータの検証を行う検証鍵は秘密にする必要はなく、これが公開されていたとしても認証方法の安全性が保たれるという長所がある。仮に証明機器の証明鍵を取り替えるものとした場合、変更された証明鍵に対応する検証鍵は証明機器から通信リンクを介して認証機器に送ればよい。このように公開鍵暗号変換を用いたチャレンジレスポンス型の認証方法は秘密鍵暗号利用の方法に比べ証明鍵を変更できる柔軟性に優れている（以上の理由により、秘密鍵、公開鍵を証明及び検証に用いた認証方法は、秘密鍵のみを証明及び検証に用いた認証方法よりも安全性が高いものとする。）。

【００１２】また同じ公開鍵暗号利用の認証方法にしても、認証方法の安全性の高さと計算機を用いて実現する場合の処理時間あるいは専用ハードウェアで実現する場合のハードウェア規模とは背反の関係にあり、さまざまな選択の可能性がある。このように公開鍵暗号利用、秘密鍵暗号利用を始め、認証方法、証明方法が複数登場しており、その何れを選択すれば良いかという選択の幅が広がっているので、映像記録装置、映像再生装置等、映像著作物関連製品の新製品を開発する際、その新製品のハードウェア規模、処理速度にとって最適な認証方法、証明方法をその新製品に実装させることができる。

【００１３】

【発明が解決しようとする課題】ところで新製品を開発する際、どの認証方法、証明方法を選択するかという自由度が増していることは、新製品をこれから開発しようとするメーカーにとって歓迎すべきことであるが、認証・証明しようとする機器の組み合わせによっては、その認証・証明が正当に行えないという不合理が発生してしまう。

【００１４】例えば公開鍵暗号利用の認証方法を有する認証機器と、秘密鍵暗号利用の認証方法を有する証明機器との組み合わせで用いる場合、これらの２つの機器は、相手側の正当性を判断できない。また、認証機器及び証明機器が互いに秘密鍵暗号利用の認証方法を行う場合でも、それを実現するソフトウェアやハードウェアのバージョン等が異なる場合、これらの２つの機器は、相手側の正当性を判断できない。

【００１５】このような事態を避けるには、多くのバージョンのチャレンジ・レスポンス型認証プロトコルを実行できる実行能力を両機器に与えればよい。例えば認証機器側に公開鍵暗号利用の第１の認証方法を実現するハードウェアと秘密鍵暗号利用の第２認証方法を実現するハードウェアとを設けておくものとする。このように設けると、証明機器側が秘密鍵暗号利用の第２証明方法のみを具備している場合でも、これらの両機器は認証、証明を行えることになる。

【００１６】しかし認証機器及び証明機器が互いに複数の認証方法及び複数の証明方法を実行できる実行能力を有している場合、両機器が安全性の低い認証処理、証明処理を自動的に行ってしまい、認証機器及び証明機器が互いに安全性の高い認証方法、証明方法のアルゴリズムを有していても、それらが活用されずに終わってしまう場合がある。例えば証明機器が公開鍵暗号利用の第１の証明方法と秘密鍵暗号利用の第２証明方法とを有する場合、認証機器及び証明機器が安全性の低い、秘密鍵暗号利用の第２認証、証明方法で認証処理をおこなってしまい、安全性が高い公開鍵暗号利用の認証方法、証明方法が生かされない場合がある。

【００１７】以上、相手側認証技術を対象に絞って説明してきたが、この問題点は相手側認証技術に限って発生するものではなく、保護すべき映像著作物を複数の機器間において送受信する必要があり、その著作権や秘密性

を保護するための暗号技術利用プロトコルが複数利用できる場合、送信側－受信側機器が用いている暗号技術利用プロトコルのバージョンが違っているため送信側において暗号化された映像著作物が正当に復号されなかったり、受信側が備えていない暗号技術利用プロトコルで送信側が映像著作物を暗号化して送信しようとしてしまうことがある。

【００１８】つまり、暗号技術利用プロトコルが複数存在することが招く「通信不能状態」は相手側認証技術に限って発生するものではなく、複数の暗号技術利用プロトコルの利用が可能な通信システムでは普遍的に発生するものといえる。本発明の目的は、複数の暗号技術利用プロトコルの利用が可能な通信システムにおいて、個々のプロトコルを有効に利用することができる通信システムを提供することである。

【００１９】

【課題を解決するための手段】上記目的は、複数の情報機器からなり、複数の暗号技術利用プロトコルの利用が可能な通信システムにおいて、各情報機器が自機の機種が複数の暗号技術利用プロトコルのうちどれとどれを利用することができる機種であるかを示す機種情報を通信すべき相手側情報機器に通知する通知手段と、相手側情報機器から機種情報が通知されると、通知された機種情報と自機の機種情報との組み合わせから情報機器間で用いるべき何れか一つの暗号技術利用プロトコルを決定する決定手段と、前記自機の機種情報に対応する１以上のプロトコルに基づいて相手側機器と通信する１以上のプロトコル対応通信部を有し、その中から決定された暗号技術利用プロトコルを用いて通信を行う通信手段とを備えることにより達成される。

【００２０】

【発明の実施の形態】以降、情報機器の実施形態として、２機の情報機器をそれぞれ認証機器－証明機器とし、これら認証機器－証明機器から構成された相手側認証システムについて説明する。本システムにおける認証機器の一例として、デジタル衛星放送にて送信された映像著作物を受信する受信装置を用いる。証明機器の一例として、映像著作物を映像記録用の光ディスクであるDVD-RAMに記録するビデオディスクレコーダを用いる。これらの機器を接続する通信リンクの一例として、所定のバス規格に準拠しており、MPEG規格に規定されたストリームデータを高速に伝送することができるAVバス１０７を用いる。不正機器として映像編集機能を具備したパーソナルコンピュータを考える。

【００２１】図１は、相手側認証システムにおける認証機器－証明機器間の接続態様を示す図である。認証機器１０１と証明機器１０４とをAVバス１０７で接続することは正当行為であるが、認証機器１０１とパーソナルコンピュータ１０８とを接続することは著作権を侵害する恐れが有る行為（不正行為とよぶ）であるものとする。何故なら、パーソナルコンピュータ１０８に映像編集を実現するソフトウェアがインストールされている場合、デジタル衛星放送にて送信された映像著作物がパーソナルコンピュータ１０８へと流出すれば、このソフトウェアの映像編集機能が悪用されて映像著作物が不正に改変されてしまうからである。

【００２２】図２は、複数の認証機器と、複数の証明機器との間の任意の接続態様を示す図である。認証機器１０１から認証機器１０３までの何れかと、証明機器１０４から証明機器１０６までの何れかとをAVバス１０７と接続する行為は正当行為であるが、図２においてはパーソナルコンピュータ１０８と接続される可能性があることは否めない。

【００２３】パーソナルコンピュータ１０８への映像著作物の流出を避けるため、認証機器１０１～認証機器１０３はAVバス１０７により何等かの機器に接続された際、その相手側の正当性を認証するものとする。認証機器１０１は、メーカーA社が開発した受信装置の上位機種であり、多くの公開鍵暗号利用アルゴリズム、秘密鍵暗号利用アルゴリズムの実現が可能であるものとする。公開鍵暗号利用認証アルゴリズムPublic_ver. 2. 6、Public_ver. 1. 3、秘密鍵暗号利用認証アルゴリズムSecret_ver. 2. 0, Secret_ver. 1. 3, Secret_ver. 1. 0による相手側認証が可能であり、多くのタイプの映像記録装置を認証できるものとする。これらの公開鍵暗号利用認証アルゴリズム、秘密鍵暗号利用認証アルゴリズムのうちアルゴリズムPublic_ver. 2. 6はその実現に複雑なハードウェアを要するもののその安全性が最も高いものとする。

【００２４】認証機器１０２は、メーカーA社が開発した受信装置の普及機種であり、認証機器１０１程ではないが、相当数の公開鍵暗号利用アルゴリズム、秘密鍵暗号利用アルゴリズムの実現が可能であるものとする。公開鍵暗号利用アルゴリズムPublic_ver. 1. 3、秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0, Secret_ver. 1. 3, Secret_ver. 1. 0による相手側認証が可能であるが、安全性が最も高い公開鍵暗号利用アルゴリズムPublic_ver. 2. 6での認証は不可能である。

【００２５】認証機器１０３は、メーカーA社が開発した受信装置の低価格機種である。ハードウェアの簡略化を追究したため、多くの証明機器との互換性を度外視しているという側面がある。秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0, Secret_ver. 1. 3が可能であり、安全性が高い公開鍵暗号利用アルゴリズムはサポートされていない。

【００２６】証明機器１０４は、メーカーA社が開発した映像記録装置の上位機種であり、多くの公開鍵暗号利用アルゴリズム、秘密鍵暗号利用アルゴリズムの実現が可能である。公開鍵暗号利用アルゴリズムPublic_ver. 2. 6、Public_ver. 1. 3、秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0、Secret_ver. 1. 3による相手側証明が可能

であり、多くのタイプの受信装置に対して自機の正当性を証明できる。

【００２７】証明機器１０５は、メーカーA社が開発した映像記録装置の普及機種であり、公開鍵暗号利用アルゴリズム、秘密鍵暗号利用アルゴリズムをそれぞれ一バージョンずつサポートしているものとする。公開鍵暗号利用アルゴリズムPublic_ver.1.3による相手側証明と、秘密鍵暗号利用アルゴリズムSecret_ver.2.0による相手側証明のみが可能であり、安全性が最も高い公開鍵暗号利用アルゴリズムPublic_ver.2.6での相手側証明は不可能である。相手側認証プロトコルの選択の余地は狭い。

【００２８】証明機器１０６は、メーカーA社が開発した映像記録装置の携帯型機種である。ハードウェアの簡略化を追究したため、Secret_ver.1.3による相手側証明のみが可能であり、相手側証明に関しては貧弱という感がある。以上のように認証機器１０１～証明機器１０６のチャレンジ・レスポンス型認証プロトコルの実行能力は機器間で違いがある。図２に示した認証機器１０１～証明機器１０６にはチャレンジ・レスポンス型認証プロトコルの実行能力の差違を示す機種コードが付されている。機種コードとは、自機の機種が複数の暗号技術利用プロトコルのうちどれとどれを実行することができる機種であるかを示すコードである。

【００２９】図３（ａ）は、図２に示す相手側認証システムにおいてどのような機種コードが存在するかを示す図である。図３（ａ）において相手側認証システム内の機種には、公開鍵暗号利用アルゴリズムPublic_ver.2.6、Public_ver.1.3、秘密鍵暗号利用アルゴリズムSecret_ver.2.0、Secret_ver.1.3、Secret_ver.1.0の実行能力を有するもの（タイプ1）、公開鍵暗号利用アルゴリズムPublic_ver.1.3、秘密鍵暗号利用アルゴリズムSecret_ver.2.0、Secret_ver.1.3、Secret_ver.1.0の実行能力を有するもの（タイプ2）、秘密鍵暗号利用アルゴリズムSecret_ver.2.0、Secret_ver.1.3の実行能力を有するもの（タイプ3）の三種が存在する。

【００３０】図３（ｂ）は、図２に示す認証機器１０１～証明機器１０６に、図３（ａ）に示す機種コードのうち、どの機種コードが付されているかを示す。次にこれらの公開鍵暗号利用アルゴリズム、秘密鍵暗号利用アルゴリズムがどのような内容であるかを図４（ａ）、図４（ｂ）、図４（ｃ）を参照しながら説明する。

【００３１】図４（ａ）はSecret_Ver1.0,1.3がどのような手順であるかを示す。Secret_Ver1.0では、認証機器は乱数rを発生し、これを検証鍵k1を用いて暗号化して得られたE(k1,r)をチャレンジデータChaとして証明機器に送信する。一方、証明機器は証明鍵k1を保有しており、前記チャレンジデータを復号して得られたD(k1,Cha)をレスポンスデータResとして認証機器に対して返す。このレスポンスデータを受信した認証機器はレスポンスデータResをチャレンジデータChaと比較し、前記チャレンジデータChaがレスポンスデータResと一致すれば送信側機器は相手側が正規の証明鍵を持つものと判断し、証明機器の正当性を認証する。

【００３２】図４（ｂ）はSecret_Ver2.0がどのような手順であるかを示す。Secret_Ver2.0では、認証機器は乱数rを発生し、これをチャレンジデータChaとして証明機器に送信する。一方、証明機器は証明鍵k1を保有しており、前記チャレンジデータを暗号化して得られたE(k1,Cha)をレスポンスデータResとして認証機器に対して返す。このレスポンスデータResを受信した認証機器はレスポンスデータResを復号して得られたD(k1,Res)をチャレンジデータChaと比較し、復号結果がチャレンジデータChaと一致すれば受信側機器は相手側が正規の証明鍵を持つものと判断し、証明機器の正当性を認証する。

【００３３】図４（ｃ）に公開鍵暗号利用アルゴリズムPublic_ver.1.3、公開鍵暗号利用アルゴリズムPublic_ver.2.6がどのような手順であるかを示す。Public_Ver1.3、2.6では、認証機器は乱数rを発生し、これをチャレンジデータChaとして証明機器に送信する。一方、証明機器は秘密鍵k1を保有しており、前記チャレンジデータを暗号化して得られたE(k1,Cha)をレスポンスデータResとして認証機器に対して返す。このレスポンスデータResを受信した認証機器はレスポンスデータResを公開鍵k2を用いて復号する。この復号結果D(k2,Res)とチャレンジデータChaとを比較し、前記復号結果がチャレンジデータと一致すれば受信側機器は相手側が正規の証明鍵を持つものと判断し、証明機器の正当性を認証する。

【００３４】図５は認証機器１０１及び証明機器１０４の内部構成を示す図である。本図を参照しながら先ず認証機器１０１の構成について説明する。認証機器１０１は図５に示すように認証機器タイプ情報格納部４と、認証モジュール群８と、認証側AVインターフェイス１１と、認証方式選択部１２と、認証方式テーブル保持部１３と、認証側制御部１４と、CSチューナー４１と、TSデコーダー４２と、AVデコーダー４３とからなる。

【００３５】認証機器タイプ情報格納部４は、機種コードを格納した不揮発性メモリである。認証機器１０１は、公開鍵暗号利用アルゴリズムPublic_ver.2.6、Public_ver.1.3、秘密鍵暗号利用アルゴリズムSecret_ver.2.0、Secret_ver.1.3、Secret_ver.1.0の実行が可能なので、図３（ｂ）を参照すれば認証機器１０１はタイプ1に属することがわかる。よって認証機器１０１の認証機器タイプ情報格納部４にはタイプ1が格納されている。

【００３６】認証モジュール群８は、図３（ａ）に示した相手側認証を実現する認証モジュールPublic_ver.2.6、Public_ver.1.3、Secret_ver.2.0、Secret_ver.1.3、Secret_ver.1.0からなる。認証モジュールPublic_ver.2.6、Public_ver.1.3は、公開の検証鍵k2を記憶するフラッシュメモリと、公開鍵検証アルゴリズムを実現す

るゲートロジックを有するハードウェアとからなる。尚、フラッシュメモリに記憶されているため、認証モジュールPublic_ver.2.6、Public_ver.1.3が記憶する公開の検証鍵k2は後日書き換えることができる。

【００３７】認証モジュールSecret_ver.2.0、Secret_ver.1.3、Secret_ver.1.0は、秘密の検証鍵k1を記憶した不揮発性メモリと、秘密鍵暗号の復号アルゴリズムを実現するゲートロジックを有するハードウェアとからなる。認証方式テーブル保持部１３は、認証機器側の機種情報及び証明機器側の機種情報の組み合わせに対応づけて、その組み合わせにおいて用いることができるチャレンジ・レスポンス型認証プロトコルを記述したテーブルを複数保持する。この複数のテーブルには、安全性優先テーブル、スピード優先テーブルといった種別が存在する。

【００３８】図６は、認証方式テーブル保持部１３が保持している安全性優先テーブルの一例を表形式で表した図である。本図を参照すれば認証機器種『タイプ1』，証明機器種『タイプ4』の組み合わせには、『公開鍵暗号利用アルゴリズムPublic_ver.2.6』が対応づけられ、認証機器種『タイプ1』，証明機器種『タイプ5』の組み合わせには、『公開鍵暗号利用アルゴリズムPublic_ver.1.3』が対応づけられていることがわかる。認証機器１０１が複数チャレンジ・レスポンス型認証プロトコルについての認証方式アルゴリズムを有していることは既に述べたが、これらのうち安全性優先テーブルは、複数のチャレンジ・レスポンス型認証プロトコルにおいて安全性が高いものを記述している。

【００３９】図７は、認証方式テーブル保持部１３が保持しているスピード優先テーブルの一例を表形式で表現した図である。本図を参照すれば認証機器種『タイプ1』，証明機器種『タイプ4』の組み合わせには『秘密鍵暗号利用アルゴリズムSecret_ver.2.0』が対応づけられ、認証機器種『タイプ1』，証明機器種『タイプ5』の組み合わせにも『秘密鍵暗号利用アルゴリズムSecret_ver.2.0』が対応づけられている。これは、スピード優先テーブルには、複数の相手側認証プロトコルにおいて処理速度が最も早いものが記述されていることを意味する。

【００４０】認証機器１０２～証明機器１０６は、認証機器１０１における方式テーブル１３と同一のものを備えている（証明機器１０４において認証機器１０１と同一の方式テーブル１３が設けられているのは、全ての認証機器、証明機器において方式テーブル１３が設けられていることを例示している。）。認証機器１０１～証明機器１０６における複数のテーブルは、認証機器１０１～証明機器１０６の方式テーブル１３において共通のシリアルナンバーによって管理されている。

【００４１】複数の認証機器、複数の証明機器において複数テーブルを共通のシリアルナンバーにて管理しているのは、これから相手側認証を行う際、どのテーブルを用いるかをその相手側に知らせるためである。尚本実施形態において、あるバージョンにおけるチャレンジ・レスポンス型認証プロトコルの実行能力を有するか否かは、そのバージョンにおける認証モジュールを実装しているか否かにより一義的に定まるものとしている。それぞれの認証モジュールが他のバージョンにおけるチャレンジ・レスポンス型認証プロトコルの実行能力を有する場合は、自機が実装している認証モジュールが実行対象としている全バージョンのチャレンジ・レスポンス型認証プロトコルを考慮して、認証方式テーブル１３を記載すべきである。

【００４２】認証方式選択部１２は、AVバス１０７を通じて認証側AVインターフェイス１１が証明機器１０４側の機種タイプ情報を受信すると、その受信した証明機器タイプと、認証機器タイプ情報格納部４に格納されている認証機器タイプとからなる組み合わせを用いて認証方式テーブル保持部１３が保持している複数のテーブルうち方式テーブルナンバーにより特定されるものから認証方式アルゴリズムを検索する。当該組み合わせに合致する認証アルゴリズムが存在すれば、その名称を読み出する共に、認証モジュール群８内の複数の認証方式モジュールのうち、読み出された認証アルゴリズムに合致するものを起動する。

【００４３】ここで認証機器１０１が証明機器側からタイプ4の機種情報を受信したとすると、認証機器１０１はタイプ1なので、タイプ1－タイプ4の組み合わせより、安全性優先テーブルから公開鍵暗号利用アルゴリズムPublic_ver.2.6での相手側認証が最適であるとの判断を行う。また認証機器１０１が証明機器側からタイプ5の機種情報を受信したとすると、タイプ1－タイプ5の組み合わせより、安全性優先テーブルから公開鍵暗号利用アルゴリズムPublic_ver.1.3での相手側認証が最適であるとの判断を行う。

【００４４】CSチューナー４１は、デジタル衛星放送の放送局が送信した搬送波をCSアンテナが受信するとこれを復調し、MPEGストリーム規格に規定されたトランスポートパケットを得てTSデコーダ４２に出力する。TSデコーダ４２は、CSチューナー４１が出力したトランスポートパケットをMPEG規格に規定されたエレメンタリィストリームに変換する。

【００４５】AVデコーダ４３は、TSデコーダー４２が出力したエレメンタリィストリームをAV信号に復号する。認証側AVインターフェイス１１は、認証モジュール群８における認証方式モジュールの何れかを用いて相手側認証を行った結果、相手側が正当な機器と判定された場合のみ、TSデコーダー４２が出力したMPEGストリームをAVバス１０７を介して証明機器１０４に送信する。不正な機器の恐れがある場合は、TSデコーダー４２が出力したMPEGストリームをAVバス１０７に送信しない。

【００４６】＜証明機器１０４＞次に証明機器１０４の構成について説明する。証明機器１０４は、方式テーブル１３と、証明機器タイプ情報格納部２４と、証明モジュール群２８と、証明側AVインターフェイス３１と、証明方式選択部３２と、証明側制御部３３と、AVデコーダ４４と、信号処理部４５と、ドライブ機構４６とからなる。

【００４７】証明機器タイプ情報格納部２４は、本証明機器におけるチャレンジ・レスポンス型認証プロトコルの実行形態がどのタイプに属するかを示す情報が格納されている。図３（ａ）においてチャレンジ・レスポンス型認証プロトコルの実行形態には、証明機器１０４のように公開鍵暗号利用アルゴリズムPublic_ver.2.6、Public_ver.1.3、秘密鍵暗号利用アルゴリズムSecret_ver.1.3、Secret_ver.2.0を実装しているもの（タイプ4）、証明機器１０５のように公開鍵暗号利用アルゴリズムPublic_ver.1.3、秘密鍵暗号利用アルゴリズムSecret_ver.2.0を実装しているもの（タイプ5）、証明機器１０６のように秘密鍵暗号利用アルゴリズムSecret_ver.1.3を実装しているもの（タイプ6）の三種が存在し、証明機器１０４はタイプ4の形態にて証明方式を実装しているので、証明機器１０４の証明機器タイプ情報格納部２４にはタイプ4が格納されている。

【００４８】証明モジュール群２８は、図３（ａ）に示した相手側証明を実現する証明モジュールPublic_ver.2.6、Public_ver.1.3、Secret_ver.2.0、Secret_ver.1.3からなる。証明モジュールPublic_ver.2.6、Public_ver.1.3は、秘密の証明鍵k1を有する記憶素子と、前記公開鍵署名作成アルゴリズムを実現するゲートロジックを有するハードウェアとからなる。

【００４９】証明モジュールSecret_ver.2.0、Secret_ver.1.3は、秘密の証明鍵k1を有する記憶素子と、前記秘密鍵暗号の暗号アルゴリズムを実現するゲートロジックを有するハードウェアとからなる。証明方式選択部３２は、AVバス１０７を介して受信した認証機器タイプと、自機が証明機器タイプ情報格納部２４にて保持している証明機器タイプとから図３（ａ）に示す証明方式選択テーブルに記載された一つの証明方式アルゴリズムを特定し、証明モジュール群２８においてアルゴリズムに対応する証明方式モジュールを起動する。

【００５０】ここで認証機器側からタイプ1の機種情報を受信したとすると、証明機器１０４はタイプ4なので、タイプ4－タイプ1の組み合わせより、安全性優先テーブルから公開鍵暗号利用アルゴリズムPublic_ver.2.6にて相手側証明方法アルゴリズムを行うべきとの判断を行う。また認証機器側からタイプ2の機種情報を受信したとすると、証明機器１０４はタイプ4なので、タイプ4－タイプ2の組み合わせより、安全性優先テーブルから秘密鍵暗号利用アルゴリズムSecret_ver.2.0での相手側証明方法アルゴリズムを行うべきとの判断を行う。

【００５１】証明側AVインターフェイス３１は、証明モジュール群２８による相手側認証により自機が正当な証明機器であることが認証機器に認められ、AVバス１０７を介して認証機器からMPEGストリームが転送されてくると、MPEGストリームを受信して信号処理部４５に出力する。

（ａ）Vデコーダ部４４は、外部から入力されてくるビデオ信号やオーディオ信号に対して所定の処理を施し、MPEGストリームに変換して信号処理部４５に出力する。

【００５２】信号処理部４５は、AVデコーダー４４から出力されたMPEGストリーム或は証明側AVインターフェイス３１が出力したMPEGストリームに増幅、波形整形、二値化、復調、エラー訂正などの処理を施して、ドライブ機構４６に出力する。ドライブ機構４６は、DVD-RAMをセットする基台と、光ピックアップとを備え、光ビームの強度を増加させて、DVD-RAM内部の情報層表面のランドを相変化させることにより信号処理部４５が出力したMPEGストリームをDVD-RAMに書き込む。

【００５３】認証側制御部１４及び証明側制御部３３は、（ｃ）ＰUと、認証機器１０１－証明機器１０４間でチャレンジ・レスポンス型認証プロトコル行う制御プログラムとからなる。図８、図９は、認証側制御部１４及び証明側制御部３３が有する制御プログラムの処理内容を示すフローチャートである。本図はまたフローチャートの各ステップにおいてどのような通信シーケンスが、認証側AVインターフェイス１１－証明側AVインターフェイス３１間で行われるかをも規定している。

【００５４】認証機器が起動されると、ステップＳ２５において認証側制御部１４は方式テーブルナンバーNxを証明機器１０４に送信する。ここで方式テーブルナンバーNxは、方式テーブル１３が保持している複数テーブルのうち、安全性優先テーブルを指示しているものとする。送信後、ステップＳ１において認証方式選択部１２に認証機器タイプTxの読み取りを行わせ、ステップＳ２においてAVバス１０７を介して認証開始信号及び認証機器タイプTxを送出をするよう認証側AVインターフェイス１１を制御する。これにより認証機器タイプ情報格納部４に格納されている認証機器タイプ1が送出される。認証側AVインターフェイス１１が認証機器タイプTxを送出すると、ステップＳ３において認証側制御部１４は証明機器タイプTyの受信待ち状態となる。

【００５５】一方証明機器が起動されると、ステップＳ２６において方式テーブルナンバーNxの受信待ちとなり、方式テーブルナンバーNxを受信すると、証明側制御部３３はステップＳ４において証明方式選択部３２に証明機器タイプTyの読み取りを行わせ、ステップＳ５において認証開始信号及び認証機器タイプTxの受信待ち状態となる。ステップＳ５の受信待ち状態において、認証側AVインターフェイス１１から認証機器タイプTxが送信されると、ステップＳ６に移行して証明機器タイプTyを認

証機器側に送出する。これにより証明機器タイプ情報格納部２４に格納されている証明機器タイプ4が証明側AVインターフェイス３１及びAVバス１０７を介して認証機器１０１に対して送出される。

【００５６】送信後、ステップＳ７において証明方式選択部３２はテーブル方式ナンバーHxに対応づけられた安全性優先テーブルから受信した認証機器タイプTxと証明機器タイプTyとに対応づけられた証明方式Hyを選択し、ステップＳ１３において証明方式Hyに相当する証明方式モジュールを起動する。ここで起動された証明方式モジュールHyが公開鍵暗号利用アルゴリズムPublic_ver. 2. 6、公開鍵暗号利用アルゴリズムPublic_ver. 1. 3ならステップＳ１７がYesとなりステップＳ８に移行して、チャレンジデータchaの受信待ちとなる。

【００５７】証明側AVインターフェイス３１が送信した証明機器タイプTyを認証側AVインターフェイス１１が受信すると、ステップＳ３において証明機器タイプTyの受信待ちを行っていた認証側制御部１４は、この情報を認証方式選択部１２に対して送出してステップＳ９に移行する。ステップＳ９において認証方式選択部１２は、ステップＳ２５において送信した方式テーブルナンバーNxに対応する安全性優先テーブルから、認証機器タイプTxと受信した証明機器タイプTyとに対応づけられた認証方式Hxを選択する。認証機器タイプ及び証明機器タイプがそれぞれタイプ1、タイプ4であるため認証方式選択部１２により公開鍵暗号利用アルゴリズムPublic_ver. 2. 6が選択される。選択後、ステップＳ１０において認証方式Hx側の認証モジュールHxとして公開鍵暗号利用アルゴリズムPublic_ver. 2. 6の認証方式モジュールを起動する。

【００５８】公開鍵暗号利用アルゴリズムPublic_ver. 2. 6の認証方式モジュールが起動されると、ステップＳ１６がYesとなり、ステップＳ１１において160ビット長の乱数Rndを生成し、これをチャレンジデータChaとして証明機器側に送信する。これにより発生された乱数はチャレンジデータとして認証側AVインターフェイス１１を介し証明機器１０４に伝送される。伝送後、ステップＳ１２においてレスポンスデータResの受信待ちとなる。

【００５９】ステップＳ８においてチャレンジデータの受信待ち状態となっていた証明側制御部３３は、証明方法アルゴリズム側AVインターフェイス３１がチャレンジデータを受信すると、ステップＳ１４に移行する。ステップＳ１４において公開鍵暗号利用アルゴリズムPublic_ver. 2. 6の認証方式モジュールは、チャレンジデータChaを一方の入力とし、秘密の証明鍵k1を他方の入力として、公開鍵署名アルゴリズムによる署名データ(k1, Cha)を作成する。

【００６０】作成された署名データは、レスポンスデータRESとして証明側AVインターフェイス３１を介して認証機器１０１に伝送される。証明機器から送信されてきたレスポンスデータRESを認証側AVインターフェイス１１が受信すると、ステップＳ１２がYes（受信した）となりステップＳ１５に移行する。ステップＳ１５では、公開鍵暗号利用アルゴリズムPublic_ver. 2. 6の認証方式モジュールにレスポンスデータの複号化を行わせ、復号結果D(k2, Res)とチャレンジデータChaとの一致判定を行うことにより証明機器側が正当なものであるかを判断させる。一致判定されれば証明機器は正当なものであると判断する。不一致と判定されれば証明機器を正当なものではないと判断する。

【００６１】以上の説明はチャレンジ・レスポンス型認証プロトコルを安全性優先テーブルから特定したが、次にチャレンジ・レスポンス型認証プロトコルをスピード優先テーブルから特定する場合について説明する。スピード優先テーブルにおいて、タイプ1－タイプ4の組み合わせには、秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0の認証方式モジュール、証明方式モジュールが対応づけられておりステップＳ１０、ステップＳ１３においてこれらが起動されたとする。

【００６２】ステップＳ１３において起動された証明方式モジュールが秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0ならステップＳ１７がNoとなるがステップＳ３３がYesとなりステップＳ２８に移行して、チャレンジデータchaの受信待ちとなる。また、秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0の認証方式モジュールが起動されると、ステップＳ１６がNoとなり、ステップＳ３２がYesとなってステップＳ２７に移行する。ステップＳ２７において64ビット長の乱数Rndを生成し、これをチャレンジデータChaとして証明機器側に送信する。これにより発生された乱数はチャレンジデータとして認証側AVインターフェイス１１を介し証明機器１０４に伝送される。伝送後、ステップＳ２９においてレスポンスデータResの受信待ちとなる。

【００６３】ステップＳ２８においてチャレンジデータの受信待ち状態となっていた証明側制御部３３は、AVインターフェイス３１がチャレンジデータを受信すると、ステップＳ３０に移行する。ステップＳ３０において証明側制御部３３は秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0の証明モジュールに、チャレンジデータChaを一方の入力とし、秘密の証明鍵k1を他方の入力として、秘密鍵署名アルゴリズムによる署名データ(k1, Cha)を作成させる。

【００６４】作成された署名データは、レスポンスデータとして証明側AVインターフェイス３１を介して認証機器１０１に伝送される。これにより符号化結果がチャレンジデータRESとして送信されることになる。証明機器から送信されてきたレスポンスデータを認証側AVインターフェイス１１が受信すると、ステップＳ２９がYes（受信した）となりステップＳ３１に移行する。ステップＳ３１では、秘密鍵暗号利用アルゴリズムSecret_ver. 2. 0の認証方式モジュールにレスポンスデータの複号

化を行わせ、復号結果D(k1,Res)とチャレンジデータChaとの一致判定を行うことにより証明機器側が正当なものであるかを判断する。

【００６５】以上の説明はチャレンジ・レスポンス型認証プロトコルをスピード優先テーブルから特定したが、最後にチャレンジ・レスポンス型認証プロトコルとして秘密鍵暗号利用アルゴリズムSecret_ver.1.3が特定された場合について説明する。方式テーブル１３が保持しているテーブルにおいて、タイプ1－タイプ4の組み合わせには、秘密鍵暗号利用アルゴリズムSecret_ver.1.3の認証方式モジュール、証明方式モジュールが対応づけられておりステップＳ１０、ステップＳ１３においてこれらが起動されたとする。

【００６６】ステップＳ１３において起動された証明方式モジュールが秘密鍵暗号利用アルゴリズムSecret_ver.1.3ならステップＳ１７、ステップＳ３３がNoとなるがステップＳ１９がYesとなりステップＳ２１に移行して、チャレンジデータchaの受信待ちとなる。また、秘密鍵暗号利用アルゴリズムSecret_ver.1.3の認証方式モジュールが起動されると、ステップＳ１６、ステップＳ３２がNoとなり、ステップＳ１８がYesとなってステップＳ２０に移行する。ステップＳ２０において64ビット長の乱数Rndを生成し、これを秘密鍵k1を用いて暗号化して得たE(k1,Rnd)をチャレンジデータChaとして証明機器側に送信する。チャレンジデータは認証側AVインターフェイス１１を介し証明機器１０４に伝送される。伝送後、ステップＳ２３においてレスポンスデータResの受信待ちとなる。

【００６７】ステップＳ２１においてチャレンジデータの受信待ち状態となっていた証明側制御部３３は、証明方法アルゴリズム側AVインターフェイス３１がチャレンジデータを受信すると、ステップＳ２２に移行する。ステップＳ２２において秘密鍵暗号利用アルゴリズムSecret_ver.1.3の認証方式モジュールは、チャレンジデータChaを一方の入力とし、秘密の証明鍵k1を他方の入力として、秘密鍵署名アルゴリズムによりD(k1,Cha)の復号を行わせ、その結果をレスポンスデータRESとして証明側AVインターフェイス３１を介して認証機器１０１に伝送する。これにより復号結果がチャレンジデータRESとして送信されることになる。

【００６８】証明機器から送信されてきたレスポンスデータを認証側AVインターフェイス１１が受信すると、ステップＳ２３がYes（受信した）となりステップＳ２４に移行する。ステップＳ２４では、秘密鍵暗号利用アルゴリズムSecret_ver.1.0の認証方式モジュールにレスポンスデータRESと乱数rとの一致判定を行わせることにより証明機器側が正当なものであるかを判断する。

【００６９】以上のように本実施例によれば、認証機器応用び証明機器の双方において複数バージョンの認証方式モジュール、複数の証明方式モジュールが利用可能である場合に、相手側機器がどのようなタイプであるかによって、相手側認証に用いるべき認証方式モジュール、証明方式モジュールを決定するので、相手側認証が正当に行なえることが保証される。

【００７０】このように認証機器の持ちうる認証方式と証明機器の持ちうる証明方式にかならず共通の方式があるようになっているため、認証機器と証明機器がどのような組み合わせであっても必ず機器認証が可能となる。安全性を優先したテーブルを設けているので、認証機器に備えられた複数バージョンの認証方式モジュール、証明機器に備えられた複数バージョンの証明方式モジュールのうち、最も安全性が高いものを相手側認証に必ず利用することができる。

【００７１】安全性優先テーブルとは別に、スピードを優先したテーブルを設けているので、認証機器に備えられた複数バージョンの認証方式モジュール、証明機器に備えられた複数バージョンの証明方式モジュールのうち、最も高速なものを相手側認証に利用することもできる。尚、本実施形態においては、認証機器及び証明機器に認証方式テーブル保持部１３を設けて、自機が用いる認証方法、証明方法を選択するようにしたが、一方側のみ方式選択のためのテーブルを設けて、その一方側に認証方法及び証明方法を決定する決定権を与えても良い（認証方法及び証明方法の組みを決定する決定権は、チャレンジ・レスポンス型認証プロトコルを決定する決定権と同義となる。）。

【００７２】この場合、決定権を有する側の機器は、相手側から機種情報を通知されると、相手側から通知された機種情報と自機の機種情報との組み合わせから認証方法－証明方法を決定する。決定後、両機では、そのプロトコルに対応する側の認証モジュール、証明モジュールを起動して、相手側の正当性を認証する。また、本実施形態においては（ａ）Ｖ機器間の接続用に規格が規定されたコネクタや通信ケーブルを一例にして説明を行ったが、機器間の接続を行うものであればコンピュータ・バス等の通信リンクを用いて良いことはいうまでもない。

【００７３】更に、チャレンジ・レスポンス型認証プロトコルではない相手側認証プロトコルに応用してもよい。チャレンジ・レスポンス型認証プロトコルではない相手側認証プロトコルとしては、一方向認証方法時系列方式がある。この方式は、認証機器、証明機器にそれぞれカウンタレジスタが備えられており、その初期値として『１』が設定されている。認証機器がリクエスト信号を証明機器に送信すると、証明機器はその設定値『１』を秘密鍵k1を用いて暗号化してその結果であるE(k1,1)を認証機器に送信する。

【００７４】送信されたE(k1,1)を受信すると、認証機器はE(k1,1)を秘密鍵k1を用いて復号して、その値と、自機のカウンタレジスタの値との一致判定を行う。両方の値が一致していれば、認証機器はカウンタレジスタの

値をインクリメントして、『２』すると共に証明機器に相手側認証が正常に行われた旨を通知する。正常判定が通知されると、証明機器がカウンタレジスタを『２』にインクリメントする。このように認証機器－証明機器のカウンタレジスタの値が『２』になったところで、上記の手順を同様に繰り返す。

【００７５】

【発明の効果】複数の情報機器からなり、複数の暗号技術利用プロトコルの利用が可能な通信システムにおいて、各情報機器が自機の機種が複数の暗号技術利用プロトコルのうちどれとどれを利用することができる機種であるかを示す機種情報を通信すべき相手側情報機器に通知する通知手段と、相手側情報機器から機種情報が通知されると、通知された機種情報と自機の機種情報との組み合わせから情報機器間で用いるべき何れか一つの暗号技術利用プロトコルを決定する決定手段と、前記自機の機種情報に対応する１以上のプロトコルに基づいて相手側機器と通信する１以上のプロトコル対応通信部を有し、その中から決定された暗号技術利用プロトコルを用いて通信を行う通信手段とを備えることにより達成される本通信システムにおいて各情報機器は通信を行う際、自機の機種情報と相手側の機種情報の組み合わせに応じて用いるべき暗号技術利用プロトコルを選択するので、処理能力やハードウェア規模が違うために暗号技術利用プロトコルの実行能力が機器間で異なっている場合でも、通信が行えることが保証される。

【００７６】例えば、自機が複数の暗号技術利用プロトコルを実行でき、相手側の情報機器が一種類の暗号技術利用プロトコルしか実行できず、暗号技術利用プロトコルの実行能力のギャップが大きい場合、複数の暗号技術利用プロトコルのうち、相手側が実行可能な一種類の暗号技術利用プロトコルを決定手段は決定するので、暗号技術利用プロトコルの実行能力のギャップの大小にかかわらず、通信が行えることが保証される。このように通信の実行が保証されるため、暗号技術利用プロトコルの実行能力のギャップが招く「通信不能状態」を未然に回避することができる。

【００７７】ここで通信システムにはn種(nは2以上の整数)の機種が存在する場合、決定手段は、n種の機種から任意の2種を選んだnC2個の機種情報の組み合わせと、各組み合わせにおいて用いるべき暗号技術利用プロトコルを示すプロトコル対応情報を対応づけたテーブルを記憶するテーブル記憶部と、n種の機種のうち、自機に合致するものの機種情報を記憶する機種情報記憶部と、相手側機器から機種情報が通知されると、テーブル記憶部が記憶しているテーブルにおいて機種情報記憶部が記憶している機種情報と、相手側機器から通知された機種情報との組み合わせに対応づけられたプロトコル対応情報が示す暗号技術利用プロトコルを前記一のプロトコルと決定する決定部とを備え、前記１以上のプロトコル対応通信部は決定部が決定した暗号技術利用プロトコルを用いて通信を行うように構成してもよい。

【００７８】この構成によれば自機及び相手側に複数の暗号技術利用プロトコルを実行できる実行能力がある場合、複数の暗号技術利用プロトコルのうち最適なものがその２つの情報機器の機種情報の組み合わせに対応づけられてテーブルに記載されていれば、２つの情報機器は、テーブルに記載された最適な暗号技術利用プロトコルを用いて通信することができる。このようにテーブルの記載次第で、２つの情報機器がどのような組み合わせであっても、その２つの情報機器にとって最適な暗号技術利用プロトコルを活用することができる。

【００７９】ここで暗号技術利用プロトコルは、相手側認証プロトコルであり、前記プロトコル対応通信部は、決定部が決定した相手側認証プロトコルにより相手側機器に正当性を証明させ、その証明結果に基づいて相手側機器が正当な情報機器であるか否かを判定する認証部と、正当な情報機器であると判定された場合のみ、保護対象となるデータを相手側情報機器に送信する送信部とを備えるように構成することができる。

【００８０】本構成によれば、デジタル化された映像著作物等、不正機器の不正行為から保護すべき保護対象データの送信能力が自機にあり、相手側の正当性確認等の責任が自機側に転嫁されている場合、その保護対象データの送信を相手側の正当性を確認してから行うので、著作権侵害行為等を未然に防止することができる。ここで前記テーブル記憶部は、nC2個の機種情報の組み合わせにおいて用いるべき相手側認証プロトコルを対応づけたテーブルを複数種別記憶しており、複数のテーブルのうち第１のテーブルには、機種情報の組み合わせにおいて用いるべき相手側認証プロトコルとして安全性が高い相手側認証プロトコルを特定するプロトコル対応情報が記述され、第２のテーブルには、機種情報の組み合わせにおいて用いるべき相手側認証プロトコルとして処理速度が高い相手側認証プロトコルを特定するプロトコル対応情報が記述されており、前記決定手段は、これから行うべき通信における安全性及び処理速度の何れか一方を考慮して、テーブル記憶部が記憶しているテーブルのうち一つを選択すると共に、どのテーブルを選択したかを相手側に通知する選択部を備え、前記決定部は、テーブル記憶部に記憶されているテーブルのうち、選択部が選択して、相手側に通知したテーブルにおける相手側認証プロトコルを決定するように構成することができる。

【００８１】この構成によれば自機及び相手側に複数の暗号技術利用プロトコルを実行できる実行能力がある場合、複数の暗号技術利用プロトコルのうち安全性が最も高いもの、処理速度が最も早いものをその２つの情報機器の機種情報の組み合わせに対応づけられてテーブルに記載しておけば、２つの情報機器は、より安全性が高い暗号技術利用プロトコル、或は、処理速度が早い暗号技

術利用プロトコルを用いて通信することができる。このようにテーブルの記載次第で、２つの情報機器がどのような組み合わせであっても、その２つの情報機器にとって最適な暗号技術利用プロトコルを利用させることができる。

【００８２】ここで複数の相手側認証プロトコルには複数のチャレンジ・レスポンス型認証プロトコルがあり、複数のチャレンジ・レスポンス型認証プロトコルには公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルと、秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルとがあり、前記第１種別のテーブルには、安全性が高いチャレンジ・レスポンス型認証プロトコルとして公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルを示すプロトコル対応情報が記述され、前記第２種別のテーブルには、処理速度が早いチャレンジ・レスポンス型認証プロトコルとして秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルを示すプロトコル対応情報が記述されており、前記１以上のプロトコル対応通信部には、公開鍵暗号利用のチャレンジ・レスポンス型認証プロトコルに基づいて通信するものと、秘密鍵暗号利用のチャレンジ・レスポンス型認証プロトコルに基づいて通信するものが存在するように構成することができる。

【００８３】このように構成それば、自機が膨大な規模のハードウェアソフトウェアとを実装することにより公開鍵暗号利用のチャレンジレスポンス型認証プロトコルとの実行能力を有している場合、その旨をテーブルに記載しておけば、公開鍵暗号利用のチャレンレスポンス型認証プロトコルとの実行能力が認証機器、証明機器の双方に存在する場合に公開鍵暗号利用プロトコルのためのハードウェア・ソフトウェアを最大限に活用することができる。

【図面の簡単な説明】

【図１】認証機器－証明機器間の接続態様を示す図である。

【図２】複数の認証機器と、複数の証明機器との間の任意の接続態様を示す図である。

【図３】（ａ）図２に示す相手側認証システムにおいてどのような機種コードが存在するかを示す図である。

（ｂ）図２に示す認証機器１０１～証明機器１０６に、図３（ａ）に示す機種コードのうち、どの機種コードが付されているかを示す図である。

【図４】（ａ）～（ｃ）公開鍵暗号利用アルゴリズム、秘密鍵暗号利用アルゴリズムがどのような内容であるかを示す図である。

【図５】本実施形態における機器認証システムの内部構成を示す図である。

【図６】認証方式テーブル保持部１３が保持している安全性優先テーブルの一例を表形式で表した図である。

【図７】認証方式テーブル保持部１３が保持しているスピード優先テーブルの一例を表形式で表現した図である。

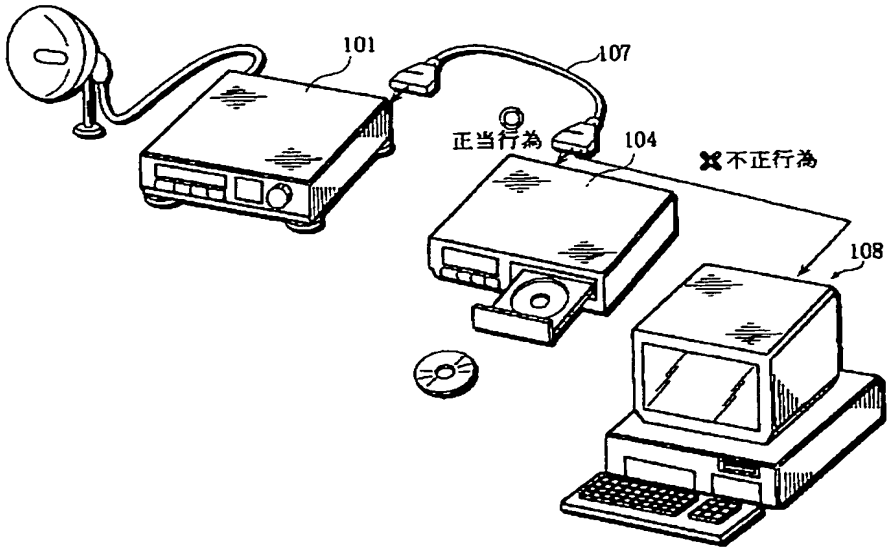
【図８】認証側制御部１４及び証明側制御部３３が有する制御プログラムの処理内容を示すフローチャートである。

【図９】認証側制御部１４及び証明側制御部３３が有する制御プログラムの処理内容を示すフローチャートである。

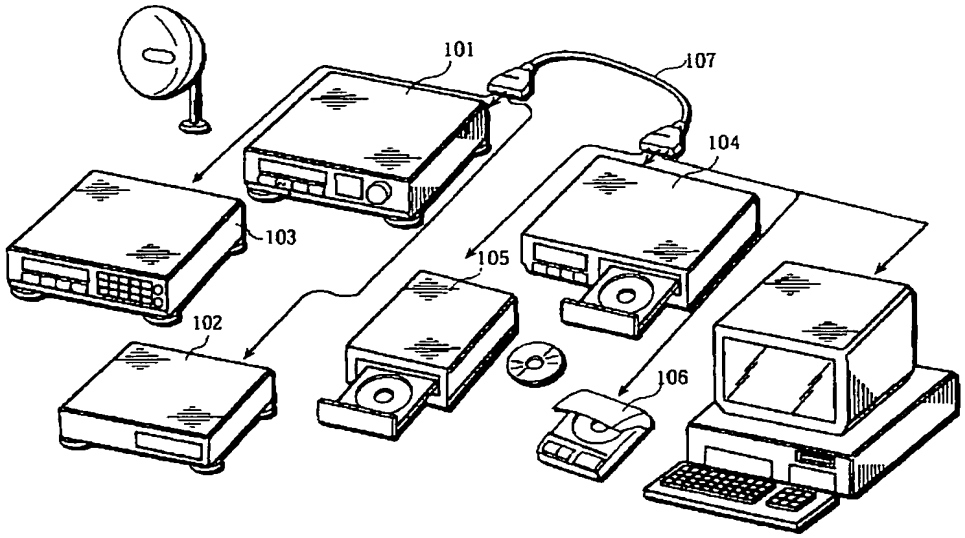
【符号の説明】

４　認証機器タイプ情報格納部
８　認証モジュール群
１１　認証側AVインターフェイス
１２　認証方式選択部
１３　認証方式テーブル保持部
１４　認証側制御部
２４　証明機器タイプ情報格納部
２８　証明モジュール群
３１　証明側AVインターフェイス
３２　証明方式選択部
３３　証明側制御部
４１　CSチューナー
４２　TSデコーダー
４３　AVデコーダー
４４　AVデコーダー
４５　信号処理部
４６　ドライブ機構
１０１　認証機器
１０２　認証機器
１０３　認証機器
１０４　証明機器
１０５　証明機器
１０６　証明機器
１０７　AVバス
１０８　パーソナルコンピュータ

【図１】



【図２】

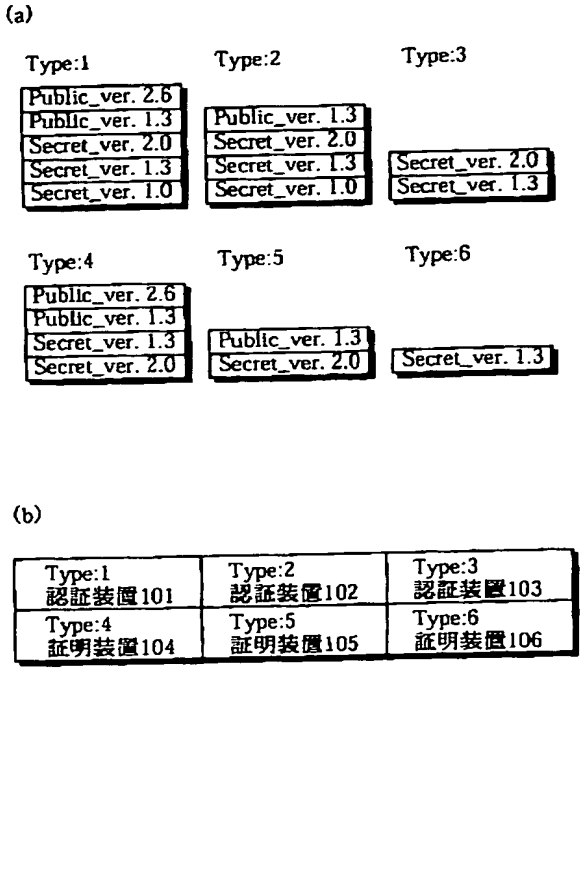


【図６】

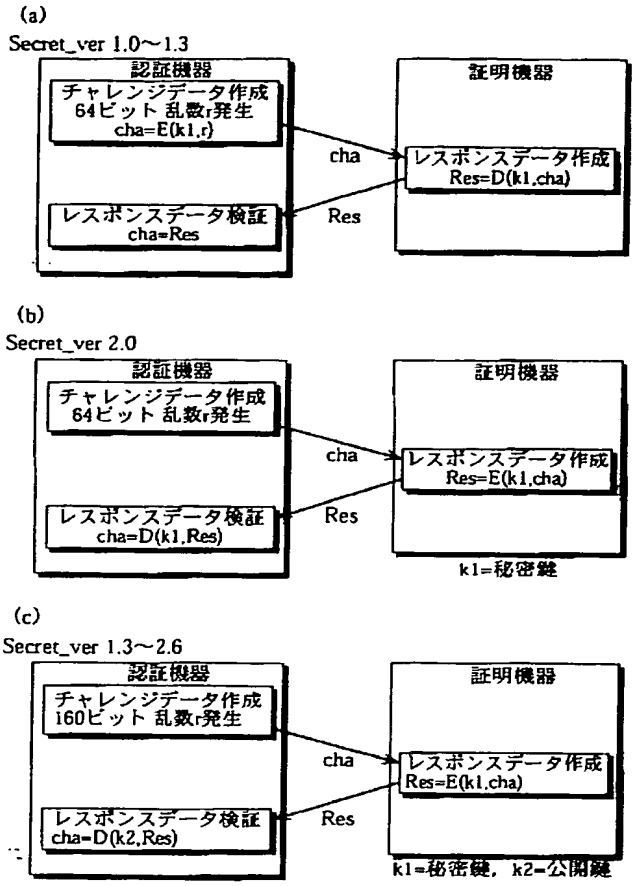
安全性優先テーブル

	Type:1	Type:2	Type:3
Type:4	Public_ver. 2.6	Secret_ver. 2.0	Secret_ver. 2.0
Type:5	Public_ver. 1.3	Public_ver. 1.3	Secret_ver. 2.0
Type:6	Secret_ver. 1.3	Secret_ver. 1.3	Secret_ver. 1.3

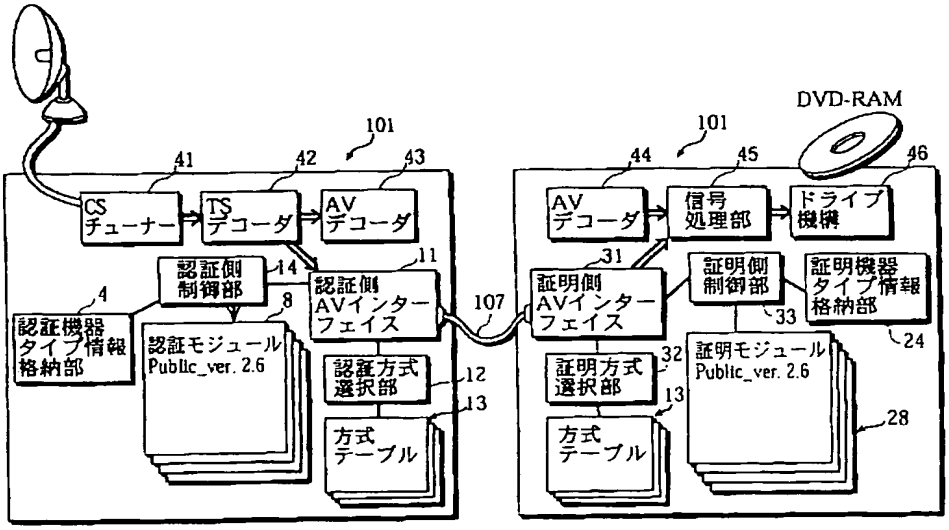
【図３】


(a)
Type:1
Public_ver. 2.6
Public_ver. 1.3
Secret_ver. 2.0
Secret_ver. 1.3
Secret_ver. 1.0
Type:2
Public_ver. 1.3
Secret_ver. 2.0
Secret_ver. 1.3
Secret_ver. 1.0
Type:3
Secret_ver. 2.0
Secret_ver. 1.3
Type:4
Public_ver. 2.6
Public_ver. 1.3
Secret_ver. 1.3
Secret_ver. 2.0
Type:5
Public_ver. 1.3
Secret_ver. 2.0
Type:6
Secret_ver. 1.3
(b)
Type:1 認証装置101
Type:2 認証装置102
Type:3 認証装置103
Type:4 証明装置104
Type:5 証明装置105
Type:6 証明装置106

【図４】


(a)
Secret_ver 1.0～1.3
認証機器
チャレンジデータ作成
64ビット 乱数r発生
cha=E(k1,r)
レスポンスデータ検証
cha=Res
cha
Res
証明機器
レスポンスデータ作成
Res=D(k1,cha)
(b)
Secret_ver 2.0
認証機器
チャレンジデータ作成
64ビット 乱数r発生
レスポンスデータ検証
cha=D(k1,Res)
cha
Res
証明機器
レスポンスデータ作成
Res=E(k1,cha)
k1=秘密鍵
(c)
Secret_ver 1.3～2.6
認証機器
チャレンジデータ作成
160ビット 乱数r発生
レスポンスデータ検証
cha=D(k2,Res)
cha
Res
証明機器
レスポンスデータ作成
Res=E(k1,cha)
k1=秘密鍵，k2=公開鍵

【図５】

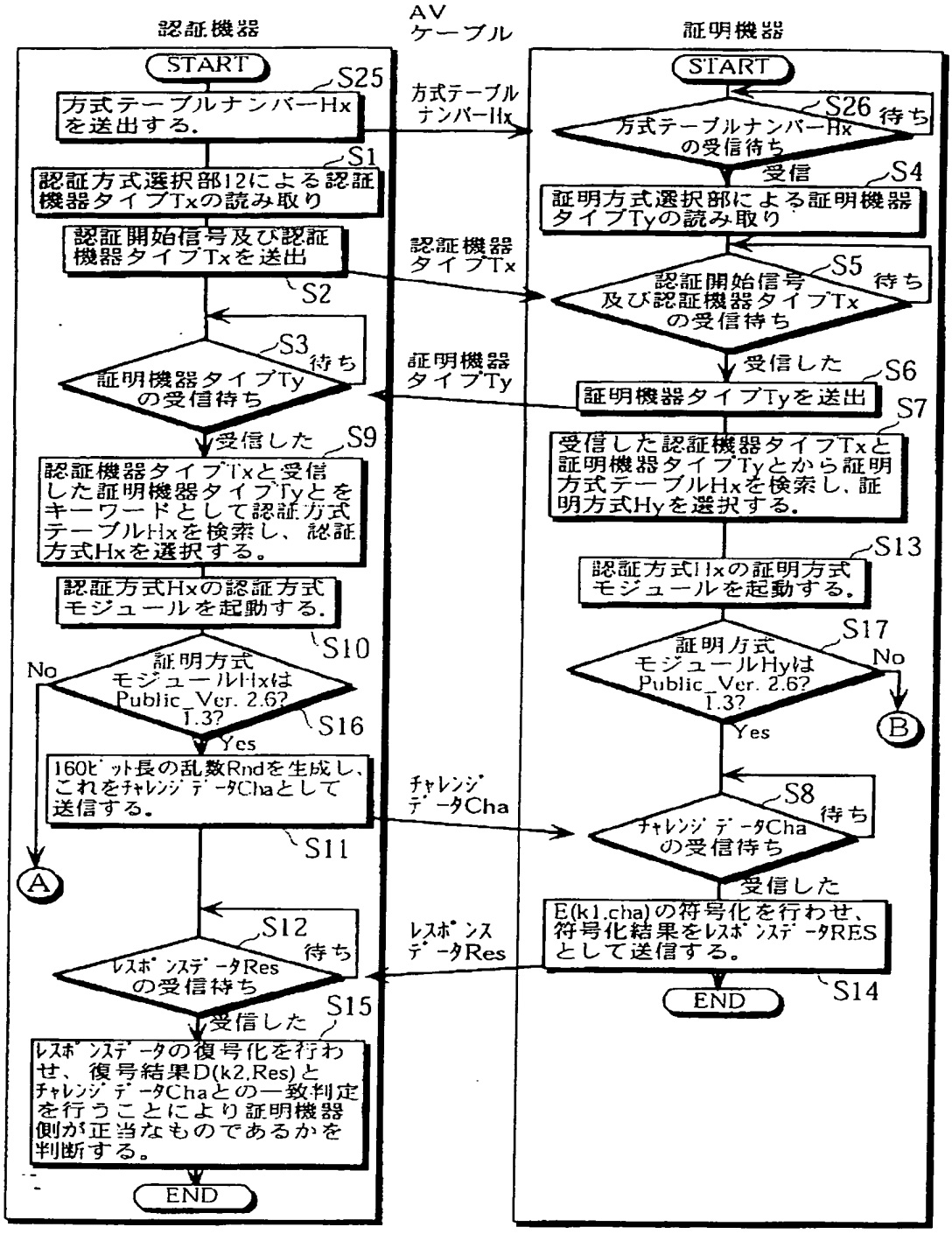

DVD-RAM
101
101
41
42
43
44
45
46
CS チューナー
TS デコーダ
AV デコーダ
AV デコーダ
信号 処理部
ドライブ 機構
認証側 制御部
14
11
認証側 AVインター フェイス
107
証明側 AVインター フェイス
31
証明側 制御部
証明機器 タイプ情報 格納部
24
4
認証機器 タイプ情報 格納部
8
認証モジュール Public_ver. 2.6
認証方式 選択部
12
13
方式 テーブル
証明方式 選択部
32
13
方式 テーブル
33
証明モジュール Public_ver. 2.6
28

【図７】

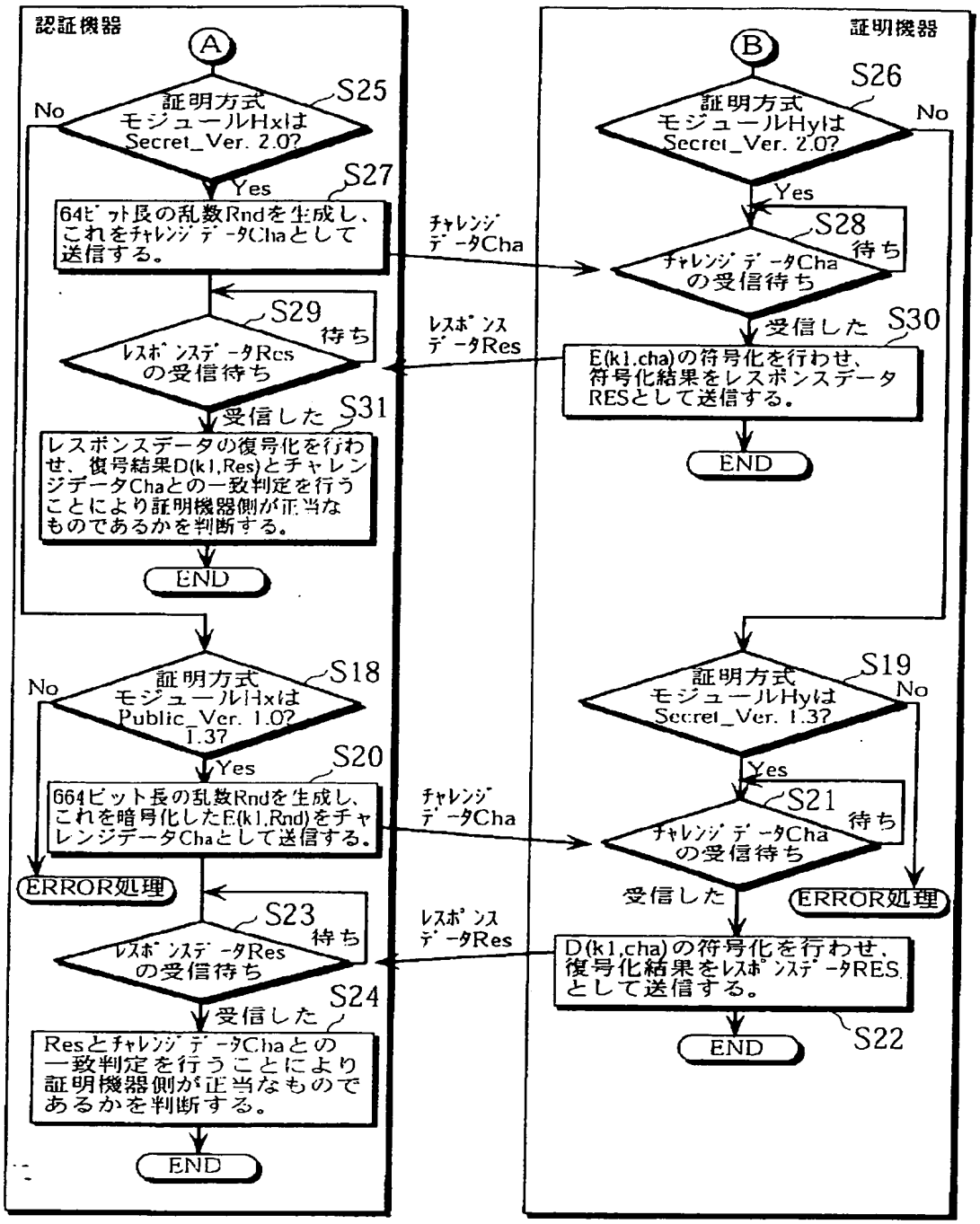
スピード優先テーブル

	Type:1	Type:2	Type:3
Type:4	Secret_ver. 2.0	Secret_ver. 2.0	Secret_ver. 2.0
Type:5	Secret_ver. 2.0	Secret_ver. 2.0	Secret_ver. 2.0
Type:6	Secret_ver. 1.3	Secret_ver. 1.3	Secret_ver. 1.3

【図８】


認証機器
AV
ケーブル
証明機器
START
S25
方式テーブルナンバーHxを送出する。
方式テーブルナンバーHx
S1
認証方式選択部12による認証機器タイプTxの読み取り
認証開始信号及び認証機器タイプTxを送出
認証機器タイプTx
S2
S3
待ち
証明機器タイプTyの受信待ち
証明機器タイプTy
受信した
S9
認証機器タイプTxと受信した証明機器タイプTyとをキーワードとして認証方式テーブルHxを検索し、認証方式Hxを選択する。
認証方式Hxの認証方式モジュールを起動する。
S10
No
証明方式モジュールHxはPublic_Ver. 2.6? 1.3?
Yes
S16
160ビット長の乱数Rndを生成し、これをチャレンジデータChaとして送信する。
チャレンジデータCha
S11
A
S12
待ち
レスポンスデータResの受信待ち
レスポンスデータRes
S15
受信した
レスポンスデータの復号化を行わせ、復号結果D(k2,Res)とチャレンジデータChaとの一致判定を行うことにより証明機器側が正当なものであるかを判断する。
END
START
S26
待ち
方式テーブルナンバーHxの受信待ち
受信
S4
証明方式選択部による証明機器タイプTyの読み取り
S5
待ち
認証開始信号及び認証機器タイプTxの受信待ち
受信した
S6
証明機器タイプTyを送出
S7
受信した認証機器タイプTxと証明機器タイプTyとから証明方式テーブルHxを検索し、証明方式Hyを選択する。
S13
認証方式Hxの証明方式モジュールを起動する。
S17
証明方式モジュールHyはPublic_Ver. 2.6? 1.3?
No
B
Yes
S8
待ち
チャレンジデータChaの受信待ち
受信した
E(k1,cha)の符号化を行わせ、符号化結果をレスポンスデータRESとして送信する。
S14
END

【図９】


認証機器
証明機器
A
B
S25
証明方式モジュールHxはSecret_Ver. 2.0?
No
Yes
S26
証明方式モジュールHyはSecret_Ver. 2.0?
No
Yes
S27
64ビット長の乱数Rndを生成し、これをチャレンジデータChaとして送信する。
チャレンジデータCha
S28
待ち
チャレンジデータChaの受信待ち
S29
待ち
レスポンスデータResの受信待ち
レスポンスデータRes
受信した
S30
E(k1,cha)の符号化を行わせ、符号化結果をレスポンスデータRESとして送信する。
END
受信した
S31
レスポンスデータの復号化を行わせ、復号結果D(k1,Res)とチャレンジデータChaとの一致判定を行うことにより証明機器側が正当なものであるかを判断する。
END
S18
証明方式モジュールHxはPublic_Ver. 1.0? 1.3?
No
Yes
S19
証明方式モジュールHyはSecret_Ver. 1.3?
No
Yes
S20
664ビット長の乱数Rndを生成し、これを暗号化したE(k1,Rnd)をチャレンジデータChaとして送信する。
チャレンジデータCha
S21
待ち
チャレンジデータChaの受信待ち
ERROR処理
受信した
ERROR処理
S23
待ち
レスポンスデータResの受信待ち
レスポンスデータRes
S24
受信した
Resとチャレンジデータ Chaとの一致判定を行うことにより証明機器側が正当なものであるかを判断する。
D(k1,cha)の符号化を行わせ、復号化結果をレスポンスデータRESとして送信する。
S22
END
END